

RL



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------|-------------|----------------------|---------------------|------------------|
| 09/519,184 | 03/06/2000 | Jukka Vialen | 324-009249-US(PAR) | 7843 |

7590 12/10/2003

Clarence A Green
PERMAN & GREEN LLP
425 Post Road
Fairfield, CT 06430

| |
|----------|
| EXAMINER |
|----------|

ZIA, MOSSADEQ

| | |
|----------|--------------|
| ART UNIT | PAPER NUMBER |
|----------|--------------|

2134

DATE MAILED: 12/10/2003

4

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/519,184

Applicant(s)

VIALEN ET AL.

Examiner

Mossadeq Zia

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 03/06/2000.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-45 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-45 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on _____ is: a) ☐ approved b) ☐ disapproved by the Examiner.
- If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

- 13) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☒ Certified copies of the priority documents have been received in Application No. 09/519,184.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
- a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 3.
- 4) ☐ Interview Summary (PTO-413) Paper No(s) _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

Art Unit: 2134

DETAILED ACTION *Claim Rejections - 35 USC § 112*

1. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

2. Claims 15, 30, 45 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter that was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. The specification does not clearly support/show the step where "new ciphering mask is produced for each interleaving period of the physical layer of the protocol stack."

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. **Claims 1, 2, 5, 9, 13, 14, 16, 17, 20, 24, 28, 29, 31, 32, 35, 39, 43, 44 are rejected under 35 U.S.C. 102(b) as anticipated by Patent. No. 5,319,712 Finkelstein et al.**
3. Regarding claims 1, 16, 31, Finkelstein discloses method of ciphering data transmission in a radio system comprising:

generating a ciphering key (session key) (col. 3, line 36-38);

producing a ciphering mask in a ciphering algorithm using the ciphering key as an input parameter (col. 3, 31-33);

producing ciphered data by applying the ciphering mask to plain data and (col. 3, line 68, col. 4, line 1);

using a logical channel specific parameter or a transport channel specific parameter (frame number) as an additional input parameter to the ciphering algorithm (Finkelstein, col. 3 line 35-37).

4. Regarding claims 2, 17, 32, Finkelstein discloses claim 1 above, and further comprising: using the direction of transmission as an additional input parameter to the ciphering algorithm (Finkelstein, fig. 1, element 124, col. 5, line 19-21).

5. Regarding claims 5, 20, 35, Finkelstein discloses claim 1 above, and further comprising: using a radio frame specific parameter (frame number structure, Finkelstein, col. 3, Table 1) as an additional input parameter to the ciphering algorithm (Finkelstein, col. 3, line 36-37, col. 4, line 65-67).

6. Regarding claims 9, 24, 39, Finkelstein discloses claim 1 above, and further discloses that the plain data includes one Radio Link Control Layer Protocol Data Unit (packet) from one logical channel, and for said logical channel an individual ciphering mask (sequence number is assigned to each packet) is produced (Finkelstein, fig. 1, element 106, 124, col. 5, line 15-17, 23-24).

7. Regarding claims 13, 28, 43, Finkelstein discloses claim 1 above, and further show that the ciphering is performed in the Medium Access Control Layer (Layer 2) of a protocol stack (Finkelstein, col. 3, line 68, col. 4, line 1).

Art Unit: 2134

8. Regarding claims 14, 29, 44, Finkelstein discloses claim 1 above, and further wherein a new ciphering mask is produced for each radio frame of the physical layer of the protocol stack. (Finkelstein, col. 3, 35-37, col. 4, col. 5, line 33-35).

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

10. **Claims 3, 4, 6-8, 10, 11, 12, 18, 19, 21, 22-23, 25-27, 33, 34, 36, 37, 38, 40-42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Patent. No. 5,319,712 by Finkelstein et al in view of Patent No. 6,535,979 by Vialen et al.**

11. Regarding claims 3, 4, 18, 19, 33, 34, Finkelstein discloses claim 1 above, but fail to disclose plurality of parameters as an additional input parameter to the ciphering algorithm.

Vialen teaches that GSM network can request user authentication at anytime during the existence of a radio bearer. The terminal can have several parallel radio bearers, and on each radio bear different ciphering parameters may be used (Vialen, fig. 9, col. 12, line 22-24).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Finkelstein as per teaching of Vialen to include different ciphering parameter to ensure diverse and efficient ciphering (Vialen, Abstract, last 2 lines).

12. Regarding claims 6, 21, 36, Finkelstein and Vialen teach claim 5, 20, 35 above, and the radio frame specific parameter is a User Equipment Frame Number (it is the Examiner's understanding that all radio equipment comes with a equipment number, therefore this limitation is a matter of choice which is encompassed by different ciphering parameter).

13. Regarding claim 7, 22, 37, Finkelstein discloses claim 1 above, but fails to disclose that the plain data includes Radio Link Control Layer Protocol Data Units from at least two parallel logical channels, and for each logical channel an individual ciphering mask is produced.

Vialen teaches a radio system where several data blocks are ciphered in parallel by the XOR method (as in GSM/GPRS), it is important that different data blocks (e.g. data from different bearers) are ciphered using different input parameters for the ciphering algorithm (Vialen, col. 2, line 45-49).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Finkelstein as per teaching of Vialen to include ciphering in parallel such that it is not possible for a hacker to listening to the transmission and knowing the structure of sent data to get a XOR from the original data and determine information of the (ciphered) data (Vialen, col. 2, line 45-49 col. 2, line 49-51).

14. Regarding claims 8, 23, 38, Finkelstein and Vialen shows claim 7, 22, 37 above, and further teaches a Radio Link Control Layer Protocol Data Unit of at least one logical channel is already ciphered, and the step of producing ciphered data is not repeated for said already ciphered Radio Link Control Layer Protocol Data Unit (Finkelstein, col. 4, line 7-8, 65-66).

15. Regarding claims 10, 25, 40, Finkelstein and Vialen discloses claim 1 above, but fails to disclose that the plain data includes at least two successive Radio Link Control Layer Protocol

Data Units of one logical channel, and for each Radio Link Control Layer Protocol Data Unit a different part of the ciphering mask is used in producing the ciphered data.

Vialen teaches a radio system where for each parallel radio bearer, a bearer specific $K_c(i)$ is used and thus the ciphering mask (the bit string) produced by the algorithm is bearer-specific (Vialen, col. 11, line 56-59).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Finkelstein as per teaching of Vialen to include ciphering in parallel such that it is not possible for a hacker to listening to the transmission and knowing the structure of sent data to get a XOR from the original data and determine information of the (ciphered) data (Vialen, col. 2, line 45-49col. 2, line 49-51).

16. Regarding claims 11, 26, 41, Finkelstein discloses claim 1 above, but fails to disclose that the plain data includes one Transport Block Set including Medium Access Control Layer Protocol Data Units of at least two different logical channels (multiplexing), and for each Transport Block Set one ciphering mask is used in producing the ciphered data.

However, Vialen teaches radio system where it is possible to multiplex several logical channels to one transport channel on the MAC layer (Vialen, col. 6, line 20-23).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Finkelstein as per teaching of Vialen to include multiplexing because ciphering and its properties can be flexibly controlled although several parallel bearers are used (Vialen, col. 2, line 42-44).

17. Regarding claims 12, 27, 42, Finkelstein discloses claim 1 above, but fails to disclose that the plain data includes one Transport Block Set including a Medium Access Control Layer

Art Unit: 2134

Protocol Data Unit of one logical channel, and for each Transport Block Set one ciphering mask is used in producing the ciphered data.

However, Vialen teaches that in a radio system one logical channel normally carries one radio bearer. A logical channel defines the service offered by a MAC layer. (Vialen, col. 6, line 13-15).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Finkelstein as per teaching of Vialen because to enhance the system is an obvious modification to the prior process taught by Finkelstein whereby "one ciphering mask is used in producing the ciphered data" becomes inherent in the system.

Conclusion

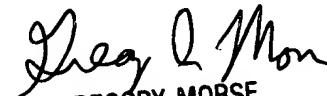
18. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Mossadeq Zia whose telephone number is 703-305-8425. The examiner can normally be reached on 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Greg Morse can be reached on 703-308-4789. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-308-3900.

Mossadeq Zia
Examiner
Art Unit 2134

mz


GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100